Arkansas Parole Board
Two Union National Plaza Building
105 West Capitol; 5th Floor
Little Rock, AR 72201-5731
(501) 682-3850 Fax: (501) 683-5381

ADMINISTRATIVE DIRECTIVE: 08-01 COMPUTER RESOURCES USE

TO: ARKANSAS PAROLE BOARD

FROM: LEROY BROWNLEE, CHAIRMAN

SUPERSEDES: Computer Resource Use AD 06-02 (Signed May 3, 2006)

APPROVED: SIGNATURE ON FILE EFFECTIVE DATE: April 15, 2008

I. APPLICABILITY. This policy applies to Arkansas Parole Board (APB) Commissioners, Hearing Examiners, support staff, contractors, volunteers, extra help, offenders, and others authorized by the Chairman to use APB computers.

II. POLICY. It is APB policy to provide use of computers and electronic services, as appropriate, and to ensure effective use of State resources. A systematic method will be used for computer hardware and software acquisition, operation, security, maintenance/upgrade, technical support, control, and repair to optimize computer resources. Computing resources are provided by APB to enhance communication, share information, increase efficiency, and perform the administrative duties of the APB and further the mission. Many of the computers and electronic services are shared with the Department of Community Correction (DCC) and the Department of Correction (ADC). They allow access to the INTERNET, electronic mail and bulletin boards, internal and external databases, library catalogs, work-related professional organizations, etc. Computers and electronic services are provided for the performance of official State business and the enhancement of the skills and knowledge necessary for such performance. Personal use of APB computers and all electronic services is strictly prohibited.

III. DEFINITIONS.

A. Computer Resources. Computers and computer related equipment, servers, local and wide area networks and input and output devices.

B. Software. Applications and programs installed on computers.

C. Computer Security. Aspects associated with providing availability, integrity, and confidentiality of information on APB computers.

D. Electronic Services. Services include, but are not limited to, access to the DCC and State networks, Internet access, electronic mail (E-Mail) and other online services.

E. Offenders. Offenders are probationers, parolees, community correction center residents, and ADC inmates.

F. Permissions. System settings that grant, deny, or limit access to various computer systems, file folders, programs, and documents.

G. User. Persons authorized access to APB computer resources.

IV. PENALTIES. Violators (Hearing Examiners and support staff) of this policy are subject to penalties ranging from verbal warnings to employment termination. Commissioners who violate this policy will be reported to the Governor's Office, by the Chairman, for appropriate action.

V. COMPUTER GUIDELINES.

A. Technical Support. Employees/Hearing Examiners/Commissioners should always use the appropriate help options and manuals provided with the computer system prior to asking for assistance. When an employee cannot resolve system or software problems, they should contact the User Support Analyst for further assistance.

Users must not allow people from outside the agency to use or attempt to fix computers unless the person is approved by the User Support Analyst to provide support or the person is known to be working as an authorized contractor or Department of Information Services (DIS) employee.

B. Planning for Computer Resources. APB provides the use of computers and electronic services to ensure effective use of State resources. A systematic method is used for computer hardware and software acquisition, operation, security, maintenance and/or upgrades, technical support, access control and repair to optimize APB and State resources. The User Support Analyst maintains the APB Information Technology Plan for maintaining computer resources consistent with budget approvals and in accordance with the Arkansas Information Systems Act 914 of 1997.

C. Ordering Computer Resources & Services. Computer purchase requests require written justification and the approval of the Chairman to ensure compatibility and consistency with the Information Technology Plan.

D. Installing Software. Software is pre-installed on computers and configured by the User Support Analyst. In order to guarantee compliance with copyright laws and insure compatibility with the DCC and the State networks, only authorized software may be installed. Users must obtain permission from the User Support Analyst before installing any software on APB computer resources. Users must not change any of the established defaults for security and/or computer access.

E. Security Measures.

1. **User Accounts.** The DCC or designee will assign user identifications (IDs). The user ID will be made available only for the period of employment with APB or as otherwise authorized by the Chairman. The DCC or APB User Support Analyst is authorized to suspend or deactivate user accounts being used for unauthorized purposes.

2. **Passwords.** Users are assigned an initial password to log into the DCC/State network, but are required to change it to a secret password known only to them. Users are required to change passwords every 90 days. Previously used passwords may not be reused until five password changes have occurred. Passwords must be at least nine characters in length and include at least three of the following four character types: UPPER CASE, lower case, special character and number. For assistance in constructing easily remembered passwords, contact the User Support Analyst.

   The combination of user ID and password uniquely identifies each user within the DCC/State network. Users must keep passwords private and must not divulge their password to any other person, including their supervisor. Users must immediately notify the User Support Analyst if they have reason to believe their password has been compromised. APB computers are configured to automatically enter a password-protected screen saver mode after 10 minutes of inactivity.

3. **Physical Security.** Supervisors and any assigned property custodian must ensure computers are in a secure location as office layout permits. Computer displays should face away from windows and doors to minimize the possibility of information being viewed by unauthorized persons.

4. **e-Mail Security/Privacy.** The use of the state electronic mail (e-Mail) is neither private nor secure. APB management has the right to access any e-Mail communication of any APB employee without their consent and/or knowledge.

5. **Supervisor's Security Responsibilities.**

   a. Monitor employee's computer resource use and take action to resolve situations of abuse.
   b. Require service/repair personnel to be properly identified and ensure the presence of an APB employee while repairs are being made.
   c. Immediately notify the User Support Analyst when a supervised employee is terminated.
   d. Take action to resolve suspected abuse. When considered appropriate, contact the next person in the supervisory chain to analyze.

6. **User Support Analyst Responsibilities.**

    a. Notify the DCC IT Administrator of any viruses and other unusual activity on the computer system.
    b. Notify the DCC IT Administrator when an employee ends their employment with the agency and insure their account is closed.
    c. Immediately notify the DCC IT Administrator when the APB suspends any account because of misuse.
    d. Conduct periodic supervisory reviews of computer and systems access permissions and notify the DCC IT Administrator when the APB makes any changes.

F. Privacy, Monitoring and Audits. Since all computers and software are APB-owned, all information stored on the computer is the property of the APB. There is no level of privacy related to the information entered, received, or transmitted. Management has the authority and capability to monitor, track, and record any and all transactions made on your computer. Monitoring is not done to intimidate or harass, rather it is to ensure proper use of computer resources. The User Support Analyst will conduct random audits of computing resources to ensure compliance with this policy.

G. Data/File Management

1. **Electronic Mail (e-Mail).** e-Mail messages may be subject to the State Record Retention policy which establishes mandatory retention periods of state documents. All employees must comply with the Record Retention policy when reviewing and retaining e-Mail communications. All retained files and electronic messages may be accessible under Freedom of Information Act (FOIA).

2. **Data Folders & Filing Documents.** 'Mission critical' data must be stored in appropriate folders located on the networked drive designated by the DCC Information Technology Section to ensure availability for all personnel who are authorized to access the folder. Data on this location is backed up and can be restored in the event of a hardware failure, whereas data stored on a local computer hard drive are not backed up and would be lost. Contact the User Support Analyst for any questions regarding folder structure and permissions setup.

    Data not intended for sharing should be stored on the networked drive designated by the DCC Information Technology Section for personal (work-related) use. This drive is viewable only to the owners and the DCC Information Technology Section but is subject to random review.

3. **Data Verification.** Employees are responsible for entering accurate data into computer systems. Supervisors must periodically check for data accuracy through routine, systematic verification techniques. Policy for specific computer systems may provide further requirements for data.

H. External Database Access. The Chairman is the sole authority for granting access to specific protected outside agency databases as appropriate and deemed necessary for an employee to perform job functions (i.e., eOMIS, ACIC/NCIC, VINES, AASIS, etc). Activity involving those databases shall be governed by the rules and regulations imposed by the agency providing access.

I. Website Changes. Only the User Support Analyst when authorized by the Chairman may make authorized changes to APB website.

J. Offender Rules Pertaining to Computer Resources. Offenders are prohibited from using any APB computer that is connected to the State network or the Internet. They are also prohibited from using any standalone machine containing personnel, agency business, or security records.

K. Computer Resource Use and Rules. Computer resources are to be used only for official State business. Upon entering the assigned user ID and password, users automatically agree to accept responsibility for and compliance with this policy and to use APB computers appropriately. Inappropriate or unacceptable use by users is the basis for disciplinary action. Although every situation that pertains to inappropriate use of APB computing resources and electronic services cannot be listed, the following is included to provide an understanding as to the type of conduct that is acceptable and unacceptable. The Chairman, or designee, reserves the right to approve or disapprove other activities which compromise APB computer systems.

1. Users shall not

a. Connect a personally owned computer to the state network.
b. Use, submit, publish, display, or transmit information which:, is defamatory, false, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory or illegal material, or violates or infringes on the rights of another person, or other statements which could cause public embarrassment to the APB.
c. Restrict or inhibit other APB users from using APB computer resources.
d. Use or attempt to use unauthorized computer resources, monitoring tools, network programs/testers, packet sniffing, remote access, key stroke recognition technology, or remote control equipment and software.
e. Use removable USB media (flash drives) or “thumb drives” without the Chairman’s approval of written justification. If approved for use, thumb drives must be encrypted and shall not be removed from the office without permission.
f. Use the system for any illegal purpose, or for personal gain.
g. Install or use “chat” or “instant messaging” software unless approved by the Chairman.
h. Use or initiate processes that degrade the efficiency of the computer system(s) such as memberships in chat rooms or receipt of streaming or broadcast audio or video via the Internet unless authorized by the User Support Analyst.

i. Mask or otherwise falsify a user's identity.
j. Modify computer configurations, installed programs or system facilities.
k. Compromise or attempt to compromise the integrity of any computer system.
l. Establish unauthorized network services including web pages, servers, FTP servers, and Telnet services.
m. Move or delete files that do not pertain to your assigned work.
n. Download or share audio (music), mp3, games, computer software or video files that could expose APB to legal claims based on copyright infringement or other legal challenges.
o. Perform any activity covered by the inappropriate use statements included in this policy.
p. Send or forward any non work-related email messages via their state e-Mail account.

2. Users must

a. Comply with written and verbal directives that address information disclosure.
b. Immediately notify management of any evidence of child pornography on any computer system. In the event of finding, or suspecting, child pornography on any APB computer system *STOP AND DO NOT TOUCH THE COMPUTER ANY FURTHER*. Immediately notify the supervisory chain and await further instructions. Do not explore the computer any further for evidence or even turn it off.
c. Immediately notify supervisors if inappropriate web pages are accidentally viewed. Failure to properly notify management will be considered intentional viewing by the user.
d. Notify their supervisor of any abnormal or suspect activities seen on computer resources. The supervisor will contact the User Support Analyst as appropriate.

VI. ATTACHMENTS

AD 08-01 Form 1 – Employee Acknowledgement

Attachment 1

Employee Acknowledgement of Computer Resources Use Policy

Please acknowledge by signing that you have received, read, and understood the Arkansas Parole Board Policy: **Administrative Directive: 08-01 Computer Resources Use** (*Supersedes Computer Resources Use AD 06-02*).

All employees or officials of the Arkansas Parole Board are responsible for complying with all pertinent policies. The Fiscal Manager will place a signed copy of this form in your personnel file.

This form must be signed and returned to the Fiscal Manger within five days after receipt of the above policy.

Employee Confirmation:

PRINT NAME	DATE	SIGNATURE
_____	_____	_____

Supervisor Confirmation:

PRINT NAME	DATE	SIGNATURE
_____	_____	_____

NOTE: This form must be signed and returned to the Fiscal Manger before an employee can use any APB computer resource.